8-10-2020

Changing the Leopard's Spots: Using Privacy Calculus to enforce ABAC access control in BYOD

Paras Bhatt
The University of Texas at San Antonio, prsbhatt9@gmail.com

Myung Ko
University of Texas, myung.ko@utsa.edu

Smriti Bhatt
Texas A & M University - San Antonio, sbhatt@tamusa.edu

Changing the Leopard's Spots: Using Privacy Calculus to enforce ABAC access control in BYOD

TREO Talk Paper

Paras Bhatt
UTSA
paras.bhatt@utsa.edu

Myung Ko
UTSA
myung.ko@utsa.edu

Smriti Bhatt
TAMUSA
sbhatt@tamusa.edu

Abstract

With the advent of smart devices (smartphones, smartwatches etc.), there has been a steep spike in the number of cyber-attacks recently. Many such attacks are orchestrated using these very smart devices as well as employees' personal devices. To safeguard against such attacks, organizations use Information Systems Security Policies (ISSP) to direct employees' behavior at the workplace. However, it is difficult to know how employees may react to such security policies. Further, employees might not be willing to allow organizations to control of their personal devices, which they might bring to the workplace under a Bring You Own Device (BYOD) policy. This study uses AWS to develop a Federated Access Control Engine (FACE - Figure 1), which includes a set of attribute based access control (ABAC) policies that regulate the BYOD devices based on their attributes (user roles, permissions etc.). With FACE organizations can manage and monitor each device that is connected to their network in real time. However, employees might be wary of letting organizations keep their personal devices in check. To resolve this we propose a privacy calculus approach where the users can learn about FACE by interacting it with in a simulated environment and also be provided complete information about the type of access control that might be placed on their device. We communicate to the users the benefits of using FACE viz. protecting their device from being used in a cyber-attack thus mitigating organizational threats. With transparent guidelines for controlling access to organizational networks we aim to reduce employee resistance to FACE. The research question we address is, how privacy calculus can facilitate widespread adoption of FACE and increase employees' trust in it (Figure 2). FACE handles requests to use any smart devices in an organization's network. Therefore, FACE provides a unique way of managing devices in organizations, restricting access to sensitive data, and preventing threats of cyberwarfare. FACE is not just an attempt to regulate devices and prevent threats but calls for better security solutions in the IS field as a whole.

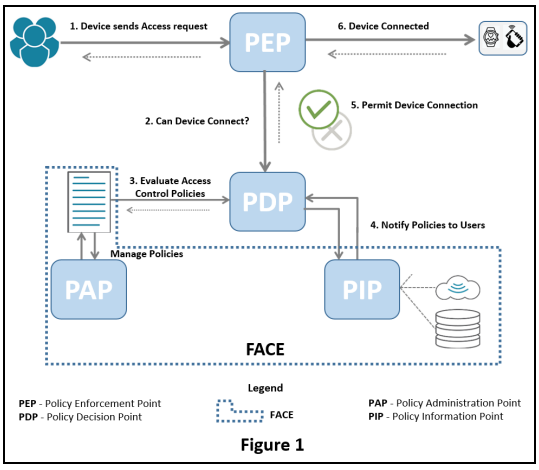

Figure 1

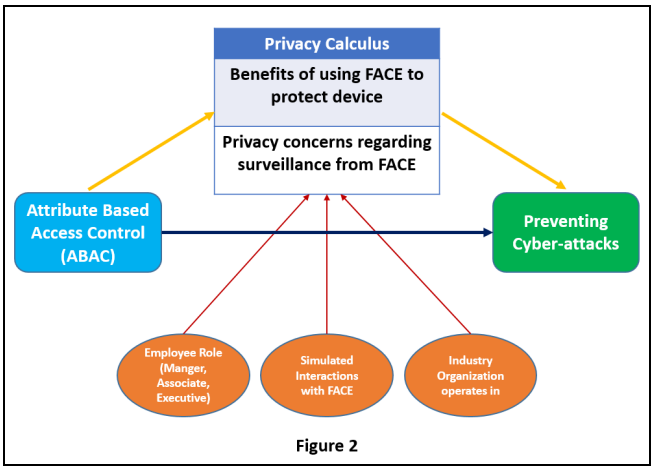

Figure 2